(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－224556
（P2003－224556A）
(43)公開日　平成15年８月８日(2003.8.8)

| (51)Int.Cl.' | 識別記号 | FI | | テーマコード'(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/08 | | Ｇ０９Ｃ　1/00 | ６４０Ｅ | ５Ｊ１０４ |
| Ｇ０９Ｃ　1/00 | ６４０ | Ｈ０４Ｌ　12/28 | ２００Ｚ | ５Ｋ０３３ |
| Ｈ０４Ｌ　12/28 | ２００ | 9/00 | ６０１Ｃ | |
| | | | ６０１Ｅ | |

審査請求　有　請求項の数28　ＯＬ　（全 18 頁）

(21)出願番号　特願2002－19135(P2002－19135)

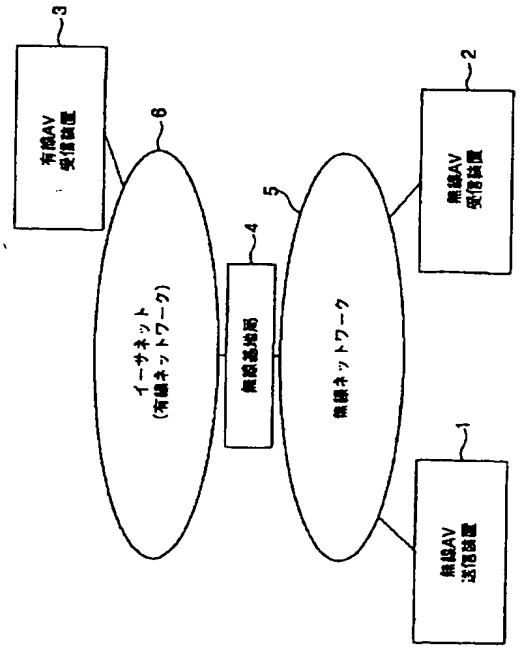
(22)出願日　平成14年１月28日(2002.1.28)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　中北　英明
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　通信装置及び通信制御方法

(57)【要約】
【課題】　著作権を保護すべきＡＶデータを暗号化して転送し復号して利用できる範囲を、一定の範囲内に制限することの可能な通信装置を提供すること。
【解決手段】　無線ＡＶ送信装置１から無線ＡＶ受信装置２へ、著作権を保護すべきＡＶデータを暗号化して、インターネットプロトコル上にて転送する。その際、著作権を保護すべきＡＶデータの暗号化や復号に使用する暗号鍵は、無線ＡＶ送信装置１と無線ＡＶ受信装置２との間で認証・鍵交換手順を行うことによって、共有される。この認証・鍵交換手順は、物理ネットワークフレーム上又はデータリンクレイヤネットワークフレーム上にて直接行なわれる。したがって、著作権を保護すべきＡＶデータをやりとりできる範囲を、ＩＰサブネット内の無線ネットワーク内、あるいはＩＰサブネット内に限定することができる。



【特許請求の範囲】

【請求項１】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、

転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、

前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、

特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、

前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項２】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、

転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、

前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、

特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、

前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項３】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、

受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、

前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、

特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、

前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項４】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、

受信された前記暗号化を施されたコンテンツ・データに対して著作権保護としての復号を施す暗号処理手段と、

前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、

特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、

前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信装置。

【請求項５】前記物理ネットワークフレームは、無線フレームであることを特徴とする請求項１または３に記載の通信装置。

【請求項６】前記データリンクレイヤネットワークフレームは、イーサネット（登録商標）フレームであることを特徴とする請求項２または４に記載の通信装置。

【請求項７】前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きの対象とするコンテンツ・データを特定するための所定の情報を、当該認証・鍵交換の手続きのためにやりとりされるデータ内に記述することを特徴とする請求項１ないし６のいずれか１項に記載の通信装置。

【請求項８】前記コンテンツ・データは、ＡＶデータ、前記ネットワークレイヤプロトコルは、インターネットプロトコルである場合に、前記所定の情報として、ＡＶストリームの送信側装置のＩＰアドレスとポート番号及び受信側装置のＩＰアドレスとポート番号の全部又は一部を用いることを特徴とする請求項７に記載の通信装置。

【請求項９】前記コンテンツ・データは、ＡＶデータ、前記ネットワークレイヤプロトコルは、インターネットプロトコルである場合に、前記所定の情報として、ＡＶストリームのＲＴＰパケットに含まれるＳＳＲＣの値を用いることを特徴とする請求項７に記載の通信装置。

【請求項１０】前記コンテンツ・データは、ＡＶデー

タ、前記ネットワークレイヤプロトコルは、インターネットプロトコルである場合に、前記所定の情報として、ＡＶストリームが転送されるＩＰパケットに含まれるフローＩＤの値を用いることを特徴とする請求項７に記載の通信装置。

【請求項１１】前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、特定のコンテンツ・データが著作権保護としての暗号化を施された上で転送されることについて送信側となる通信装置から受信側となる通信装置へ通知する手続きを含むことを特徴とする請求項７に記載の通信装置。

【請求項１２】前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含み、

前記コンテンツ・データは、前記著作権保護用制御データを含まずに転送されるものであることを特徴とする請求項７に記載の通信装置。

【請求項１３】著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施して転送する機能を有する通信装置であって、

転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、

前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、

前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信装置。

【請求項１４】著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、

受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、

前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、

前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信装置。

【請求項１５】前記著作権保護用制御データは、暗号管理情報又は暗号再計算タイミングの少なくとも一方を含むものであることを特徴とする請求項１２ないし１４のいずれか１項に記載の通信装置。

【請求項１６】前記コンテンツ・データの処理を行なうコンテンツ・データ処理手段を更に備えたことを特徴とする請求項１ないし１５のいずれか１項に記載の通信装置。

【請求項１７】前記ネットワークレイヤプロトコルは、インターネットプロトコルであることを特徴とする請求項１ないし１６のいずれか１項に記載の通信装置。

【請求項１８】前記コンテンツ・データは、ＡＶデータであることを特徴とする請求項１ないし１７のいずれか１項に記載の通信装置。

【請求項１９】著作権を保護すべきコンテンツ・データに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを受信し、

前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信制御方法。

【請求項２０】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置における通信制御方法であって、

前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを送信し、

前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする通信制御方法。

【請求項２１】著作権を保護すべきコンテンツ・データ

であって著作権保護用制御データを含まないものに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、
前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を受信する第１のステップと、
前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第２のステップとを有し、
前記第２のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信制御方法。
【請求項２２】著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置における通信制御方法であって、
前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を送信する第１のステップと、
前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第２のステップとを有し、
前記第２のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする通信制御方法。
【請求項２３】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、
転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理機能と、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、
前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、
特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース機能としてコンピュータを実現させ、
前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なわせるためのプログラム。
【請求項２４】著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、
転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理機能と、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、
前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、
特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース機能としてコンピュータを実現させ、
前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なわせるためのプログラム。
【請求項２５】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、
受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理機能と、
前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、
特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース機能としてコンピュータを実現させ、
前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なわせるためのプログラム。
【請求項２６】著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、
受信された前記暗号化を施されたコンテンツ・データに対して著作権保護としての復号を施す暗号処理機能と、
前記コンテンツ・データの送信側となる通信装置との間

で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理機能と、
特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース機能としてコンピュータを実現させ、
前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なわせるためのプログラム。
【請求項２７】著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施して転送する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、
転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理機能と、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、
前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きであって、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むものを行なう認証・鍵交換処理機能とをコンピュータに実現させるためのプログラム。
【請求項２８】著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置としてコンピュータを機能させるためのプログラムであって、
前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理機能と、
受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理機能と、
前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きであって、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むものを行なう認証・鍵交換処理機能とをコンピュータに実現させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権保護機能を持ってＡＶデータのやり取りを行なう通信装置及び通信制御方法に関する。
【０００２】
【従来の技術】デジタル情報家電と呼ばれる商品が増加している。これらは、デジタル放送の開始などに伴い、普及が期待される商品群であり、デジタル放送対応テレビや、セットトップボックス、デジタルＶＴＲ、ＤＶＤプレーヤ、ハードディスクレコーダ等、デジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。
【０００３】この際、考慮すべきは著作権保護である。デジタルデータは、コピー時の品質劣化が無いなどの利点が強調される反面、不正コピーが容易であるなどの欠点も持つ。
【０００４】このため、デジタルＡＶ機器同士をつなぐデジタルネットワークであるＩＥＥＥ１３９４には、認証・鍵交換機構や、データの暗号化の機能を兼ね備えられている。
【０００５】
【発明が解決しようとする課題】ここで、ある送信装置から、著作権を保護すべきＡＶデータ（ただし、暗号化したもの）を、受信装置に転送する場合を考える。当該ＡＶデータをやりとりする範囲（ただし、受信装置が復号できる範囲）は、一定の範囲内（例えば、当該ＡＶデータを使用できる正当な権限の範囲内（例えば、著作権３０条の私的使用の範囲内）あるいはそれよりもさらに狭い範囲内）に制限され、そのような範囲を越えてのＡＶデータのやりとりは（視聴料や著作権料等の支払いが伴うようにするなどの措置を考えない限りは）できないようにされるのが望ましい。
【０００６】一定の範囲内でのＡＶデータのやり取りの典型的な例は、ＩＥＥＥ１３９４や無線ネットワーク等のホームネットワークに閉じた通信である。
【０００７】一定の範囲内を越えたＡＶデータのやり取りの典型的な例は、「公衆網（例えば、インターネットや、電話網等）」を介したやり取りである。
【０００８】近い将来、デジタルネットワークの種類は、無線、パソコンネットワーク等と、色々な種類に増加するものと考えられるが、これらの多くでは著作権保護は考慮されていないのが現状である。
【０００９】また、ネットワークはローカルなものから、グローバルなものまで幅広くあり、著作権保護の観点からは明確に区別されるのが望ましい。
【００１０】本発明は、上記事情を考慮してなされたもので、著作権を保護すべきコンテンツ・データを暗号化して転送し復号して利用できる範囲を、一定の範囲内に制限することの可能な通信装置及び通信制御方法を提供することを目的とする。
【００１１】
【課題を解決するための手段】本発明は、著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施さ

れたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする。

【００１２】本発明は、著作権を保護すべきコンテンツ・データに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、前記受信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【００１３】本発明は、著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定の物理ネットワークとのインタフェースとなる物理ネットワークインタフェース手段とを備え、前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上にて直接行なうことを特徴とする。

【００１４】本発明は、著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して著作権保護としての復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段と、特定のデータリンクレイヤネットワークとのインタフェースとなるデータリンクレイヤネットワークインタフェース手段とを備え、前記送信側となる通信装置との間での前記認証・鍵交換の手続きのためのデータのやりとりを、前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【００１５】本発明は、著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施して転送する機能を有する通信装置であって、転送対象となる前記コンテンツ・データに対して著作権保護として暗号化を施す暗号処理手段と、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、前記コンテンツ・データの受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【００１６】本発明は、著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置であって、前記著作権保護としての暗号化を施されたコンテンツ・データの転送を所定のネットワークレイヤプロトコル上にて行うための転送処理手段と、受信された前記暗号化を施されたコンテンツ・データに対して復号を施す暗号処理手段と、前記コンテンツ・データの送信側となる通信装置との間で、前記著作権保護としての前記暗号化及び前記復号のための認証・鍵交換の手続きを行なう認証・鍵交換処理手段とを備え、前記認証・鍵交換処理手段により行われる前記認証・鍵交換の手続きは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【００１７】本発明は、著作権を保護すべきコンテンツ・データに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを受信し、前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のため

の認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【００１８】本発明は、著作権保護としての暗号化を施されたコンテンツ・データを受信し復号する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を直接搭載した物理ネットワークフレーム又はデータリンクレイヤネットワークフレームを送信し、前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを、前記物理ネットワークフレーム上又は前記データリンクレイヤネットワークフレーム上にて直接行なうことを特徴とする。

【００１９】本発明は、著作権を保護すべきコンテンツ・データであって著作権保護用制御データを含まないものに暗号化を施してネットワークレイヤプロトコル上にて転送する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの受信側となる通信装置から、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きを行なうことの要求を受信する第１のステップと、前記受信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第２のステップとを有し、前記第２のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【００２０】本発明は、著作権保護としての暗号化を施されたコンテンツ・データであって著作権保護用制御データを含まないものを受信し復号する機能を有する通信装置における通信制御方法であって、前記著作権保護としての暗号化を施されたコンテンツ・データの送信側となる通信装置へ、前記著作権保護としての暗号化及び前記復号のための認証・鍵交換の手続きを行なうことの要求を送信する第１のステップと、前記送信側となる通信装置との間で、前記著作権保護としての暗号化及び該受信側となる通信装置での復号のための認証・鍵交換の手続きのためのデータのやりとりを行なう第２のステップとを有し、前記第２のステップは、当該認証・鍵交換の手続きの対象とするコンテンツ・データに対する著作権保護用制御データの全部又は一部を交換する手続きを含むことを特徴とする。

【００２１】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００２２】本発明によれば、著作権を保護すべきコンテンツ・データを暗号化して転送し復号して利用できる範囲を、一定の範囲内（例えば、同一のＩＰサブネット内における１つの無線ネットワーク内、同一のＩＰサブネット内）に制限することができる。

【００２３】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００２４】図１に、本実施形態のネットワークシステムの構成例を示す。

【００２５】図１は、ある家庭の家庭ネットワークと、これに接続されたネットワーク機器を示している。もちろん、図１に示したネットワーク機器以外に、他のネットワーク機器や、その他の装置が存在しても構わない。

【００２６】図１に例示されるように、この家庭には、家庭ネットワークとして、イーサネット（有線ネットワーク）６と無線ネットワーク５が存在し、これらが無線基地局（無線アクセスポイント）４で相互接続されている。この無線基地局４は、ブリッジ（イーサネットブリッジ）の役割を果たす。無線ネットワーク５上でも、イーサネットフレーム（あるいは、これに順ずる形）で、パケットは転送されるものとする（ただし、これに限定するものではない）。例えば、ＩＥＥＥ８０２．１１ａや、ＩＥＥＥ８０２．１１ｂ等の無線ＬＡＮがこれにあたる。さらに、無線ネットワーク５には、無線ＡＶ送信装置１と、無線ＡＶ受信装置２が、イーサネット６には有線ＡＶ受信装置３が、それぞれ接続されている。

【００２７】無線ＡＶ送信装置１と、無線ＡＶ受信装置２との間では、ＡＶデータのやり取りを行なう。無線ＡＶ送信装置１と、有線ＡＶ受信装置３との間についても同様である。無線ＡＶ送信装置１は、セットトップボックスやＤＶＤプレーヤ等といったＡＶデータのソースデバイスとなり得る機器であり、無線ＡＶ受信装置２や有線ＡＶ受信装置３は、テレビやディスプレイ、スピーカ、あるいは録画・録音装置といった、ＡＶデータのシンクデバイスとなり得る機器である。

【００２８】図２に、無線ＡＶ送信装置１の内部構成例を示す。

【００２９】図２に示されるように、無線ＡＶ送信装置１は、ＡＶデータの生成や蓄積を行い、ネットワークに送出するＡＶデータのソースとなるＡＶデータ生成／蓄積部１１、タイムスタンプ処理やシーケンス番号処理

等、これらのＡＶデータのトランスポートレイヤ層の処理を行なうＲＴＰ処理部１２、これらのパケットをＴＣＰ／ＩＰのパケットで送受信するＴＣＰ／ＩＰパケット送受信部１３、暗号化等の著作権保護の処理が必要なデータに関して、ＡＶデータの暗号化処理を行なう著作権保護暗号化部１４、イーサネットフレームを送受信するイーサネットフレーム送受信部１５、ＩＰアドレスとイーサネットアドレスの対応を取るためのＩＰ／イーサネットアドレス対応テーブル１６、著作権保護のために、ＡＶ受信装置との間で認証や鍵交換等を行なうための著作権保護認証・鍵交換部１７、無線ネットワークとのインタフェース部（無線ネットワークＩ／Ｆ部）１８を備えている。

【００３０】図３に、無線ＡＶ受信装置２の内部構成例を示す。

【００３１】図３に示されるように、無線ＡＶ受信装置２は、無線ネットワークとのインタフェース部（無線ネットワークＩ／Ｆ部）２８、イーサネットフレームを送受信するイーサネットフレーム送受信部２５、著作権保護のために暗号化されて転送されてきたＡＶデータを復号化する著作権保護復号化部２４、これらのパケットをＴＣＰ／ＩＰのパケットで送受信するＴＣＰ／ＩＰパケット送受信部２３、タイムスタンプ処理やシーケンス番号処理等、これらのＡＶデータのトランスポートレイヤ層の処理を行なうＲＴＰ処理部２２、受信したＡＶデータの再生や蓄積（録音や録画）を行い、ＡＶデータのシンクとなるＡＶデータ再生／蓄積部２１、ＩＰアドレスとイーサネットアドレスの対応を取るためのＩＰ／イーサネットアドレス対応テーブル２６、著作権保護のために、ＡＶ送信装置との間で認証や鍵交換等を行なうための著作権保護認証・鍵交換部２７を備えている。

【００３２】また、図４に、有線ＡＶ受信装置３の内部構成例を示す。

【００３３】図４に示されるように、イーサネットに接続される有線ＡＶ受信装置３は、基本的には、図３の無線ＡＶ受信装置２と同様の構成を有する（なお、イーサネットに接続されることから、図３の無線ネットワークインタフェース部の代わりに、イーサネットインタフェース部（イーサネットＩ／Ｆ部）３８を有する）。ただし、後述するように、無線ＡＶ受信装置２が無線ＡＶ送信装置１との間で行なう著作権保護のための認証や鍵交換の少なくとも一部は、無線制御フレーム上にてやり取りがなされる。このため、有線ＡＶ受信装置３は無線制御フレームをやり取りする機能を持たないことから、著作権保護認証・鍵交換部３７でやり取りされる著作権保護用の制御データは、無線ＡＶ受信装置２のそれと異なり、イーサネットフレームなり、ＩＰパケットなりの形で転送される点も、無線ＡＶ受信装置と相違する点である。

【００３４】次に、本実施形態の家庭ネットワークシステムにおいてやり取りされるパケットのフォーマットについて説明する。

【００３５】ＴＣＰ／ＩＰパケットは、無線ネットワーク５、イーサネット６の両方のネットワークにおいて、どちらもイーサネットフレームにカプセル化されて転送される。ネットワークがイーサネットの場合は、このイーサネットフレーム（イーサネットヘッダ＋ＴＣＰ／ＩＰパケット）の形でパケットが転送される。一方、ネットワークが無線ネットワークの場合には、上記のイーサネットフレームに、さらに無線レイヤヘッダが付与される形で、（無線レイヤヘッダ＋イーサネットヘッダ＋ＴＣＰ／ＩＰパケット）の形で転送される。なお、トレイラについてはプロトコルに準ずればよい（トレイラを使用するプロトコルであってもよいし、そうでないプロトコルであってもよい）。

【００３６】図５に、無線レイヤフレームのフォーマットの一例を示す。

【００３７】無線レイヤヘッダには、無線ネットワーク５上でのみ使用する制御データ（例えば、８０２．１１無線ＬＡＮにおけるＦＣフィールドや、Ｄｕｒ／ＩＤフィールド等）等が含まれる。このＦＣフィールドには、２ビットのＴｙｐｅフィールドが含まれており、無線レイヤフレームの種類が示される。Ｔｙｐｅフィールドが０ならば管理用、１ならば制御用、２ならば通常データ用である。管理用無線レイヤフレームとして代表的なものは、ビーコンであり、周期的にネットワークに配信されて、各無線ＡＶ装置の無線レイヤにおけるクロックを調整するために、主に使用される。そのほか、プローブ要求および応答、認証関係構築および解消、ネットワークへの参加要求および応答などがある。一方、制御用無線レイヤフレームには、送信期間設定に関するもの、受信確認に関するものなどがある。

【００３８】上記著作権保護用の制御データは、管理用無線レイヤフレーム、制御用無線レイヤフレーム、または、Ｔｙｐｅフィールドが３であるような新たな種類の無線レイヤフレームのいずれかによって扱うことができ、後述の著作権保護シーケンスに適用可能である。

【００３９】どの種類のフレームでも、ＦＣフィールドに、４ビットのＳｕｂＴｙｐｅフィールドがさらに含まれており、現在はリザーブされているＳｕｂｔｙｐｅを、著作権保護用として設定すれば、各装置で、著作権保護用制御データを識別できる。後述する認証・鍵交換要求および認証・鍵交換手順で利用することが可能である。

【００４０】さて、以下では、本実施形態の動作について説明する。なお、著作権保護の仕組みとしては、例えばＤＴＣＰ（Ｄｉｇｉｔａｌ　ＴｒａｎｓｍｉｓｓｉｏｎＣｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）の仕組みを用いた場合を想定して説明する（なお、他の著作権保護の仕組みを用いても構わない）。ＤＴＣＰについては、

ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍに詳しい。

【００４１】図６に、本家庭ネットワークにおけるシーケンス例を示す。なお、図７に、無線ＡＶ送信装置１の認証・鍵交換に関する手順の一例を示し、図８に、無線ＡＶ受信装置２の認証・鍵交換に関する手順の一例を示す（なお、以下の各シーケンス例についても、無線ＡＶ送信装置１及び有線ＡＶ受信装置３の認証・鍵交換に関する手順の一例は、図７及び図８と同様である）。

【００４２】ここでは、無線ＡＶ受信装置２が、無線ＡＶ送信装置１に対して、ＡＶデータの送信を要求する場合を例にとって考える。このとき、例えばＡＶ／Ｃプロトコル（１３９４トレードアソシエーションが規定した、ＡＶ機器制御用のコマンド、及びそのプロトコル）や、ＲＴＳＰ（ＩＥＴＦが規定した、ＷｅｂサーバのＡＶストリーミング機能の遠隔制御用のプロトコル）を使って、ＴＣＰ／ＩＰ上にてコマンド（プロトコル）のやり取りを行なう（Ｓ１）。

【００４３】すると、無線ＡＶ送信装置１は、上記コマンドを受け付け、無線ＡＶ受信装置２に対して、ＡＶデータの送信を開始する（Ｓ２，Ｓ３，Ｓ１２１）。このＡＶデータの送信は、ＴＣＰ／ＩＰのパケット（あるいはＵＤＰ／ＩＰのパケットでも良い）にて行なわれる。実際には、図９に示すように、転送されるＡＶデータは、ＲＴＰ（リアルタイムトランスポートプロトコル）（ＩＥＴＦにて標準化された、ＡＶデータ転送用の転送プロトコル）にて転送されても良い。ここで、送信するデータは、著作権保護により保護すべきＡＶデータであるとする。この場合、ＲＴＰにて転送されるＡＶデータは、暗号化がなされた上で転送される（Ｓ２）。また、ＲＴＰパケットには、ＣＣＩ（コピー制御情報）や、暗号管理情報、暗号再計算タイミング等の著作権保護用制御データが付与された形で、（暗号化された）ＡＶデータが転送される。

【００４４】これを受信した無線ＡＶ受信装置２は、受信したＡＶデータに暗号がかけられていることを発見しあるいはＡＶデータが暗号化されて転送されてくることを事前に察知するなりして（Ｓ１０１）、無線ＡＶ送信装置１に対して、暗号鍵（ここでは、暗号鍵＝復号鍵とする）の入手を試みるべく認証・鍵交換手順を要求し（Ｓ４，Ｓ１０２，Ｓ１２２）、これを契機として、無線ＡＶ送信装置１と無線ＡＶ受信装置２との間で、認証・鍵交換手順を行う（Ｓ５，Ｓ１０３，Ｓ１２３）。

【００４５】この際の認証・鍵交換の要求（Ｓ４）及び実際の認証・鍵交換手順（Ｓ５）は、図５にあるようなＴＣＰ／ＩＰパケット上で行なわれるのではなく、図１０にあるように、無線レイヤフレームに、ＡＫＥ（認証・鍵交換）用のデータが直接搭載される形にて行なわれる。この無線レイヤヘッダのうち、「その無線レイヤフレームが、どのようなプロトコルのためのフレームであるか」を表示するフィールドとして、著作権保護プロトコルであること（例えば、ＤＴＣＰであること）を意味する数値が入ることにしても良い。このようにすることにより、著作権保護（ＡＫＥ）用のフレームが転送されていることが、受信側のノードは認識することができるようになる。

【００４６】また、このＡＫＥ手順は、無線レイヤフレームを用いて行なわれるため、このＡＫＥ手順が無線ネットワーク５内に留まって処理されることが確実に保証される。

【００４７】つまり、かりにＴＣＰ／ＩＰパケットにてＡＫＥ手順を行なう場合を考えると、その場合には、隣の家同士や長距離あるいは国境を越えて（ＴＣＰ／ＩＰパケットが届くので）ＡＫＥパケットを交換することができるようになり、例えば著作権法３０条の私的使用の範囲を越える範囲でのＡＶデータの転送（コピーを含む）がなされてしまう場合があり得る。

【００４８】これに対して、本実施形態のようにＡＫＥ手順を無線レイヤフレームを用いて行なうことで、ＡＫＥがなされる最大範囲は、同一の無線ネットワーク上の中に留まることが保証される。なぜなら、無線レイヤフレームは、無線ネットワークを越えて転送されることが出来ないからである。

【００４９】もちろん、この仕組みを強固にするために、「ＡＫＥ手順を転送している無線フレームは、必ず、対向側のネットワークにブリッジ接続しない」という無線基地局やブリッジ装置を作成すると、上記の保証をより完全に行なうことが出来る。

【００５０】さて、上記の認証・鍵交換手順が終了すると、無線ＡＶ送信装置１と無線ＡＶ受信装置２との間にて、暗号鍵の値の共有が行なえる状態になっていることを意味する。繰り返すと、この状態（２つのノード間で暗号鍵の値が共有できる状態）は、同じ無線ネットワーク５に接続されたノード同士に限定される。つまり、無線ＡＶ送信装置１と無線ＡＶ受信装置２との間では、無線レイヤ制御パケットの転送が可能なので、上記ＡＫＥ手順が成立することが可能である。一方、無線ＡＶ送信装置１と有線ＡＶ受信装置３との間では、ＡＫＥのためのパケット（フレーム）のやりとりが、無線ＡＶ送信装置１から見て、無線基地局４から向こう側（無線基地局から、有線ＡＶ受信装置間）では不可能であるため、ＡＫＥ手順が成功することがない。このことから、著作権保護が通用する区間を「無線ネットワーク内（それも、１つのＩＰサブネット内）」という形に限定することが可能となる。

【００５１】このようにして、「無線ネットワークをこえたＡＫＥ、ひいては不当なＡＶデータの転送」を未然に防ぐことが可能となる。

【００５２】さて、上記では、無線レイヤフレーム上で直接ＡＫＥ用のデータのやり取りを行なうことで、著作権保護の仕組み（正式なＡＶデータ受信装置が、受信し

た暗号化ＡＶデータの復号化ができる仕組み）が有効である範囲を、無線ネットワーク内に限定することが可能であった。

【００５３】これに代えて、著作権保護の仕組みが有効である範囲を、「イーサネットフレームが届く範囲」と限定することも可能である。

【００５４】これは、図１１のように、ＡＫＥ制御データの転送を、イーサネットフレーム上にて直接行なうことによって、実現可能である。つまり、イーサネットフレームが、イーサネットパケットが届く範囲内の、ＩＰサブネット内と限定することが可能であるため、（ＴＣＰ／ＩＰパケットを用いる代わりに）このイーサネットフレームを用いてＡＫＥ手順を行なえば、このＡＫＥが成立する範囲を、イーサネットフレームが届く範囲（通常、ブリッジ接続を許容した１つのＩＰサブネット内）と限定することが可能となる。

【００５５】図１２に、このような場合のシーケンス例を示す。

【００５６】図１２のように（なお、前述したように、この場合の無線ＡＶ送信装置１及び有線ＡＶ受信装置３の認証・鍵交換に関する手順の一例は、図７及び図８と同様である）、無線ネットワーク５上の無線ＡＶ送信装置１と、イーサネット６に接続された有線ＡＶ受信装置３との間でのＡＫＥのやり取りも可能となる。この場合は、ＩＰルータを越えてＡＫＥのやり取りが転送されることを未然に防ぐことが可能であるため、著作権保護されたＡＶデータの届く範囲（暗号が復号化されてしまう範囲）を、イーサネットフレームが転送される同一サブネット内に限定することが可能になる。

【００５７】もちろん、この仕組みを強固にするために、「ＡＫＥ手順を転送しているイーサネットフレームは、必ず、異なるサブネットワークにルーティングしないしない」というルータ装置を作成すると、上記の保証をより完全に行なうことが出来る。

【００５８】なお、例えば、図１の例においては、無線ＡＶ送信装置１は、認証・鍵交換手順に無線レイヤフレームのみを用いる構成を採用することも、イーサネットフレームのみを用いる構成を採用することも、無線レイヤフレームとイーサネットフレームを適宜選択して使用する構成を採用することも可能である。

【００５９】また、図６や図１２の手順において、ＡＶデータ転送が開始された後に認証・鍵交換要求及び認証・鍵交換手順を行ったが、ＡＶデータ転送が開始される以前に認証・鍵交換要求及び認証・鍵交換手順を行う構成も可能である。また、図６や図１２の手順において、ＡＶデータの転送が完了してから、認証・鍵交換要求及び認証・鍵交換手順を行うようにしてもよいし、ＡＶデータの転送の途中で、認証・鍵交換要求及び認証・鍵交換手順を行うようにしてもよい。また、図６や図１２の手順において、認証・鍵交換要求及び認証・鍵交換手順に成功した後に、あらためて暗号化されたＡＶデータを最初から転送する構成も可能である。また、図６や図１２の手順において、認証・鍵交換要求や認証・鍵交換手順において、一方の装置から他方の装置にあるメッセージを出し、該他方の装置から該一方の装置に該あるメッセージに対する応答を返す際に、該一方の装置が該あるメッセージを出してからこれに対する該応答を受けるまでの時間が、予め定められた基準時間を超える場合には、該認証・鍵交換要求や認証・鍵交換手順を中止するようにしてもよい。これらの点は、以下の各シーケンス例についても同様である。

【００６０】さて、以下では、無線レイヤフレームもしくはイーサネットフレーム上にて送信装置と受信装置との間でやり取りされる認証・鍵交換（ＡＫＥ）手順のバリエーションを説明する。

【００６１】なお、以下では、無線レイヤフレームもしくはイーサネットフレームのいずれかを用いるものとする。図１の例の場合、無線ＡＶ受信装置２に対しては、無線レイヤフレームとイーサネットフレームの両方が使用でき、有線ＡＶ受信装置３に対しては、イーサネットフレームが使用できる。

【００６２】また、ここでは、無線ＡＶ受信装置２と有線ＡＶ受信装置３を総称して、ＡＶ受信装置と呼ぶものとする。

【００６３】ＡＫＥは、特定のＲＴＰストリームによって転送されるＡＶストリームに関して行なわれるものである。このため、ＡＫＥを行なう前提として、「どのＡＶストリームに関するＡＫＥなのか」についての交渉を行なう必要がある場合がある。例えば、ＡＶ受信装置が、受信したＡＶストリームが暗号化されていることを認識し、「このＡＶストリームについてのＡＫＥをさせて欲しい」と無線ＡＶ送信装置に問い合わせる場合がある。また、無線ＡＶ送信装置が、「このＡＶストリームは、暗号化してＡＶ受信装置に対して送出する。このことを、予め、あるいは、ＡＶストリーム転送と同時に、ＡＶ受信装置に対して通知し、ＡＫＥのトリガをかけさせる必要がある」と判断し、ＡＶ受信装置に対して、「このＡＶストリームは暗号化して送信する。よって、このＡＶストリームについてＡＫＥ手順を自装置（無線ＡＶ送信装置）に対して行なうべし」という通知を行なう場合が考えられる。

【００６４】もちろん、１本１本のＡＶストリーム毎にＡＫＥを行なうのではなく、「無線ＡＶ送信装置と、ＡＶ受信装置との間でやり取りされる、全てのＲＴＰストリームに関して有効とするためのＡＫＥ」を一度に行なってしまい、その後は、無線ＡＶ送信装置とＡＶ受信装置との間でやり取りされる全てのＲＴＰストリームに関しても、このＡＫＥ手順により定められた条件に従って、ＡＶデータの暗号化が行なわれるようになっていても良い。

【００６５】その場合、どのポート番号の通信においては、どのような著作権保護制御情報（暗号管理情報や暗号再計算タイミング等）を用いるものであるかについての情報交換を行ってもよい。

【００６６】図１３に、ＡＶ受信装置（２あるいは３）側が、無線ＡＶ送信装置１に対してＡＫＥのトリガを最初にかける場合についてのシーケンスの例を示す。

【００６７】なお、無線ＡＶ送信装置のＩＰアドレスをａ、送信ポート番号を＃ｘとし、ＡＶ受信装置のＩＰアドレスをｂ、受信ポート番号を＃ｙとする。

【００６８】こでまでの手順と同様に、ＡＶ受信装置から無線ＡＶ送信装置へ、ＡＶ制御コマンドが出され、無線ＡＶ送信装置は、ＡＶデータを暗号化して、ＡＶ受信装置へ転送する（Ｓ２１、Ｓ２２，Ｓ２３）。

【００６９】ここで、ＡＶ受信装置は、何らかの方法で、受信したＡＶストリームが暗号化されていることを認識する。例えば、「受信したＡＶストリームを複号しても、所望のＡＶストリームが再生できない場合」、あるいは「受信したＡＶストリームに、図９に示したような著作権保護用の制御データが付属しており、これを検出して、そのＡＶストリームが暗号化されていることを認識する場合」等が考えられる。

【００７０】受信したＡＶストリームが暗号化されていること、あるいはその可能性があることを認識したＡＶ受信装置は、認証・鍵交換要求を無線ＡＶ送信装置に対して送出する（Ｓ２４）。なお、前述したように、これを、無線レイヤパケットを使って行なう場合と、イーサネットフレームを使ってこれを行なう場合が可能である。なお、そのプロトコルフィールドの値として、例えば「ＤＴＣＰ」を意味する値を持つようにしても良い。すなわち、この手順もＤＴＣＰの手順の一部とすることが可能である。

【００７１】その際、ＡＶ受信装置は、そのＡＫＥ要求（あるいは、後続のＡＫＥ手順パケット）にて、「どのＡＶストリームについてのＡＫＥであるか」を明示する。例えば、無線ＡＶ送信装置のＩＰアドレスとポート番号及びＡＶ受信装置のＩＰアドレスとポート番号を、そのＡＫＥ要求に明記する（Ｓ２４参照）。また、対象とするＡＶストリームを特定する他の方法として、ＲＴＰのＳＳＲＣフィールドの値（ＡＶソース毎に一意につけられる識別番号であり、例えば、ＲＴＰのスペックであるＲＦＣ１８８９に詳しい）を用いて、この番号をＡＫＥ要求に明記しても良い。また、ＩＰｖ６パケット等に含まれる「フローＩＤ」の値を用いても良い。その他の方法も可能である。

【００７２】また、この要求に、暗号管理情報や暗号再計算タイミング等についての情報が含まれていてもよい。

【００７３】また、無線ＡＶ送信装置と、ＡＶ受信装置との間には、複数のＡＶストリーム（例えば、映像と音声）が同時にやり取りされている場合があるので、この「どのＡＶストリームについてのＡＫＥであるか」についての情報（例えば、送信装置と受信装置のＩＰアドレスとポート番号の組の情報、又はＳＳＲＣの値やフローＩＤの値、又はこれらの組み合わせ）に、一度に複数のＡＶストリームを指定できるようになっていても良い。

【００７４】このようなＡＫＥ要求を受信した無線ＡＶ送信装置は、そのＡＫＥ要求（あるいは、ＡＫＥ手続き）が、どのＡＶストリームのためのものであるかを認識した上で、ＡＫＥ手順を継続する（Ｓ２５）。

【００７５】結局、ＡＫＥ手順が終了すると、ＡＶ受信装置は、そのＡＫＥ結果をもとに、その暗号化ＡＶストリームの復号鍵を取得（あるいは、復号鍵を取得するための計算のための初期情報を取得）することが可能になる（Ｓ２６）。

【００７６】次に、図１４に、無線ＡＶ送信装置１側が、ＡＶ受信装置（２あるいは３）に対して、あるＡＶストリームについて、「このＡＶストリームは暗号化して送信する」旨を通知し、これをトリガとして、ＡＶ受信装置が無線ＡＶ送信装置に対してＡＫＥ要求をかける場合についてのシーケンスの例を示す。

【００７７】Ｓ３１～Ｓ３３については、図１３のシーケンス例のＳ２１～Ｓ２３と同様である。

【００７８】このシーケンス例では、無線ＡＶ送信装置は、ＡＶ受信装置に対して送信するＡＶストリームが、ＤＴＣＰ等のプロトコルに従って暗号化され、これをＡＶ受信装置が復号するには、無線ＡＶ送信装置との間でＡＫＥを行なう必要があることをＡＶ受信装置に対して通知する（Ｓ３４）。この通知は、ＩＰパケットを用いて行なっても良いが、このシーケンス例では、その後で行われるＡＫＥ手順と同様に、無線レイヤパケットもしくはイーサネットフレームを用いて行なわれるものとする。

【００７９】Ｓ３４～３６は、図１３のシーケンス例のＳ２３～Ｓ２５と同様である。

【００８０】すなわち、受信するＡＶストリームあるいは受信したＡＶストリームが暗号化されることを認識したＡＶ受信装置は、認証・鍵交換要求を送信装置に対して送出する（Ｓ３５）。ＡＫＥ要求を受信した無線ＡＶ送信装置は、そのＡＫＥ要求（あるいは、ＡＫＥ手続き）が、どのＡＶストリームのためのものであるかを認識した上で、ＡＫＥ手順を継続する（Ｓ３６）。ＡＫＥ手順が終了すると、ＡＶ受信装置は、そのＡＫＥ結果をもとに、その暗号化ＡＶストリームの復号鍵を取得（あるいは、復号鍵を取得するための計算のための初期情報を取得）することが可能になる（Ｓ３７）。

【００８１】さて、ここまでの説明では、従来のＤＴＣＰと同様に、転送されるＡＶストリームには、図９と同様に、著作権保護用の制御データが付与されることを想定していた。この著作権保護用の制御データは、例え

ば、そのＡＶストリームの暗号管理情報（例えば、そのＡＶストリームが、コピー自由（ｃｏｐｙ　ｆｒｅｅ）であるか、１回コピー可能（ｃｏｐｙ　ｏｎｃｅ）であるか、更なるコピーは不可であるか（ｎｏ　ｍｏｒｅ　ｃｏｐｙ）、コピー不可（ｎｅｖｅｒ　ｃｏｐｙ）であるかについての情報）や、暗号鍵の再計算タイミング（例えば、どのＲＴＰシーケンス番号のときに特定の暗号鍵を使用しはじめ、続いて同シーケンス番号のいくつおきに、暗号鍵を再計算すべきか、についての情報）を通知するためのフラグ等が含まれる。ところが、場合によっては、転送されるＡＶストリームに、著作権保護用の制御データを付与できない場合（つまり、ＲＴＰパケットをそのまま転送する必要がある場合）が考えられる。

【００８２】図１５、このような場合のＡＶストリームの転送フォーマットの例を示す。

【００８３】図１５の例は、基本的には、図９から、著作権保護用制御データを取り去ったもの、すなわち通常のＲＴＰパケット（ただし、そのペイロードのＡＶストリームが暗号化されたもの）のフォーマットとなる。

【００８４】このような場合には、事前に（あるいは、該ＡＶストリーム転送中に）、「そのＡＶストリームの暗号管理情報」や、「何パケット毎に、ＡＶストリームの暗号鍵を再計算すべきか」についての情報を、前述のＡＫＥ手順中で行なえばよい。

【００８５】図１６に、この場合のシーケンス例を示す。

【００８６】例えば、無線ＡＶ送信装置が、転送するＡＶストリームについての暗号管理情報や、ＡＶストリーム暗号鍵の再計算タイミングを、ＡＫＥ手順中にて、ＡＶ受信装置に対して通知する（Ｓ４３参照）。

【００８７】このようにすることにより、転送されるＡＶストリームに著作権保護用の制御データを付与しなくても、送信側と受信側で、暗号管理情報や、暗号鍵の再計算のタイミングを予め共有することが可能となり、ひいては、送信側から受信側に対して、セキュアなＡＶストリームの転送を実現することが可能になる。

【００８８】図１６では、ＡＶ受信装置からトリガがかかる例であるが、もちろん無線ＡＶ送信装置からＡＶ受信装置に対して最初に通知する場合においても、同様に行なうことが可能である（例えば、図１４のシーケンス例のＳ３６において行うことが可能である）。

【００８９】なお、図１では、無線ＡＶ送信装置が存在したが、その代わりにまたはそれに加えて、同様の機能をする有線ＡＶ送信装置が存在してもよい（有線ＡＶ送信装置の構成例は、図２のインタフェースを修正したものである；この修正は、図３の無線ＡＶ受信装置から図４の有線ＡＶ受信装置への修正と同様である）。ただし、有線ＡＶ送信装置は、無線レイヤフレームを使用できないので、イーサネットフレーム上で認証・鍵交換を行う機能を有することになる。したがって、図１においては、有線ＡＶ送信装置は、無線ＡＶ受信装置と有線ＡＶ受信装置のいずれとも認証・鍵交換を行うことができることになる。

【００９０】また、図１では、イーサネット（有線ネットワーク）と無線ネットワークが存在したが、無線ネットワークのみ存在してもよい。この場合、無線ＡＶ送信装置と無線ＡＶ受信装置との間で、無線レイヤフレーム上で認証・鍵交換を行うことができる（なお、イーサネットフレーム上で認証・鍵交換を行ってもよい）。あるいは、逆に、イーサネット（有線ネットワーク）のみ存在してもよい。この場合、有線ＡＶ送信装置と有線ＡＶ受信装置との間で、イーサネットフレーム上で認証・鍵交換を行うことができる。

【００９１】また、例えば、図１のイーサネットに、更に他の異なる（１又は複数の）無線基地局及び無線ネットワークが接続されていてもよい。あるいは、図１の無線ネットワークに、更に他の異なる（１又は複数の）イーサネットが接続されていてもよい。家庭ネットワークの構成がどのようになっていても、無線レイヤフレームあるいはイーサネットフレームの到達する範囲内でのみ、認証・鍵交換を行うことができる。

【００９２】なお、以上で想定したプロトコルは、一例であり、同様の性質を持つ他のプロトコルについても本発明は適用可能である。

【００９３】また、以上では、ローカルエリアネットワークとして家庭ネットワークを例にとって説明したが、もちろん、企業内網など他のローカルネットワークであっても本発明は同様に適用可能である。

【００９４】また、以上では、ＡＶコンテンツの暗号処理について、暗号鍵＝復号鍵を想定して説明したが、暗号鍵≠復号鍵となる場合にも、本発明は適用可能である。

【００９５】なお、以上の各機能は、ソフトウェアとして実現可能である。また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムとして実施することもでき、該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【００９６】なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能

である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。また、この発明の実施の形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【００９７】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００９８】

【発明の効果】本発明によれば、著作権を保護すべきコンテンツ・データを暗号化して転送し復号して利用できる範囲を、一定の範囲内に制限することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るネットワークシステムの構成例を示す図

【図２】同実施形態に係る無線ＡＶ送信装置の構成例を示す図

【図３】同実施形態に係る無線ＡＶ受信装置の構成例を示す図

【図４】同実施形態に係る有線ＡＶ受信装置の構成例を示す図

【図５】同実施形態に係る無線レイヤフレームのフォーマットの一例を示す図

【図６】同実施形態に係るネットワークシステムの全体のシーケンスの一例を示す図

【図７】同実施形態に係る無線ＡＶ送信装置の認証・鍵交換に関する手順の一例を示すフローチャート

【図８】同実施形態に係る無線ＡＶ受信装置及び有線ＡＶ受信装置の認証・鍵交換に関する手順の一例を示すフローチャート

【図９】同実施形態に係るＩＰパケットによるＡＶデータ転送フォーマットの一例を示す図

【図１０】同実施形態に係る認証・鍵交換用データの転送方法の一例について説明するための図

【図１１】同実施形態に係る認証・鍵交換用データの転送方法の他の例について説明するための図

【図１２】同実施形態に係るネットワークシステムの全体のシーケンスの他の例を示す図

【図１３】同実施形態に係るネットワークシステムの全体のシーケンスのさらに他の例を示す図

【図１４】同実施形態に係るネットワークシステムの全体のシーケンスのさらに他の例を示す図

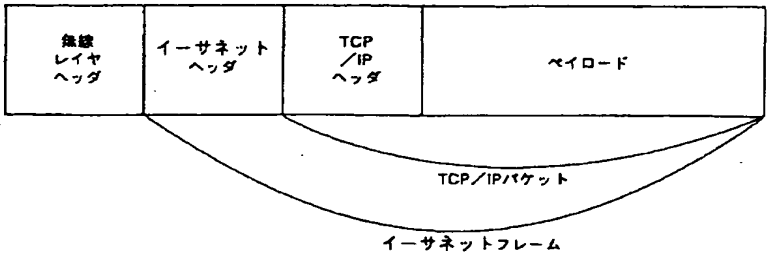
【図１５】同実施形態に係るＩＰパケットによるＡＶデータ転送フォーマットの他の例を示す図

【図１６】同実施形態に係るネットワークシステムの全体のシーケンスのさらに他の例を示す図

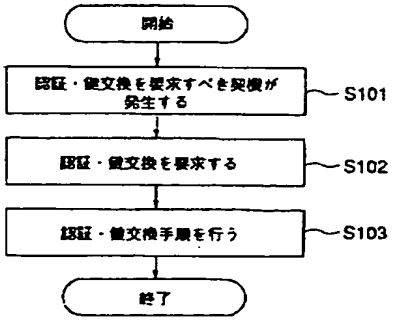
【符号の説明】

１…無線ＡＶ送信装置
２…無線ＡＶ受信装置
３…有線ＡＶ受信装置
４…無線基地局
５…無線ネットワーク
６…イーサネット
１１…ＡＶデータ生成／蓄積部
１２，２２，３２…ＲＴＰ処理部
１３，２３，３３…ＴＣＰ／ＩＰパケット送受信部
１４，２４，３４…著作権保護暗号化部
１５，２５，３５…イーサネットフレーム送受信部
１６，２６，３６…ＩＰ／イーサネットアドレス対応テーブル
１７，２７，３７…著作権保護認証・鍵交換部
１８，２８…無線ネットワークＩ／Ｆ部
２１，３１…ＡＶデータ再生／蓄積部
３８…イーサネットＩ／Ｆ部

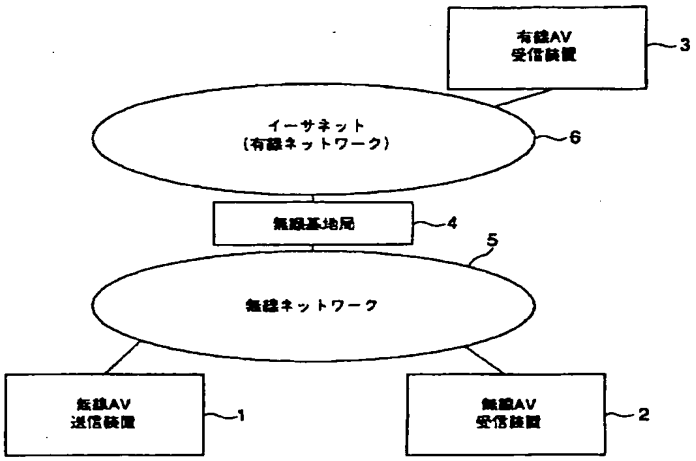
【図５】



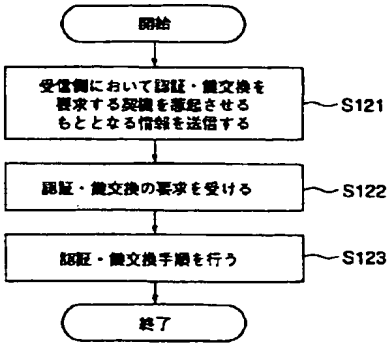

【図７】



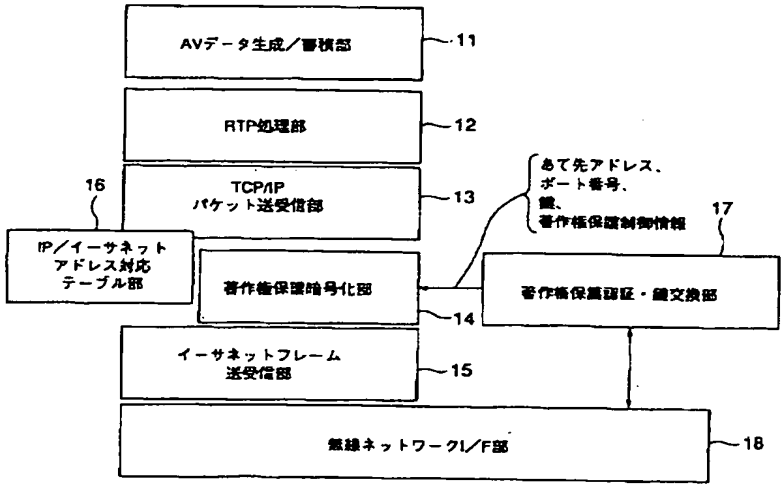
【図１】




【図８】

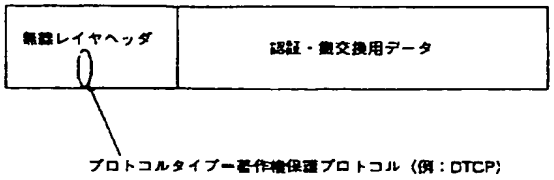



【図２】

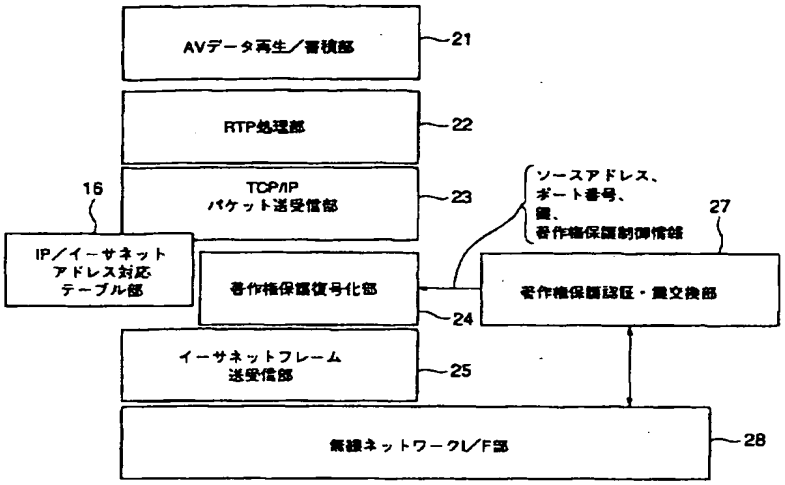



【図９】

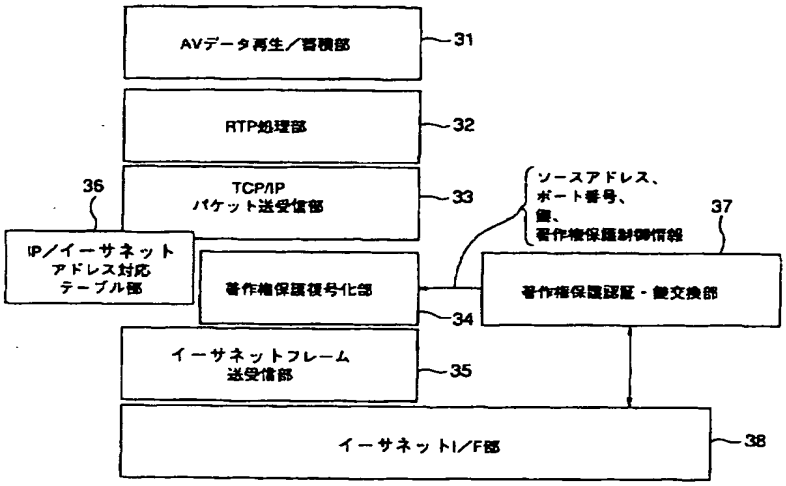

【図１０】



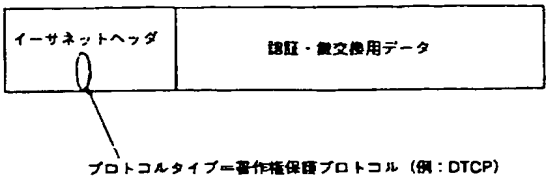
【図３】


AVデータ再生／蓄積部
21
RTP処理部
22
TCP/IP
パケット送受信部
23
16
IP／イーサネット
アドレス対応
テーブル部
著作権保護復号化部
24
ソースアドレス、
ポート番号、
鍵、
著作権保護制御情報
27
著作権保護認証・鍵交換部
イーサネットフレーム
送受信部
25
無線ネットワークI/F部
28

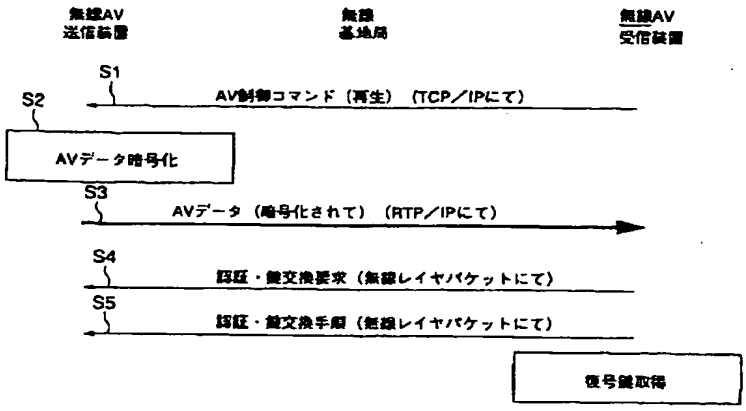
【図４】


AVデータ再生／蓄積部
31
RTP処理部
32
TCP/IP
パケット送受信部
33
36
IP／イーサネット
アドレス対応
テーブル部
著作権保護復号化部
34
ソースアドレス、
ポート番号、
鍵、
著作権保護制御情報
37
著作権保護認証・鍵交換部
イーサネットフレーム
送受信部
35
イーサネットI/F部
38

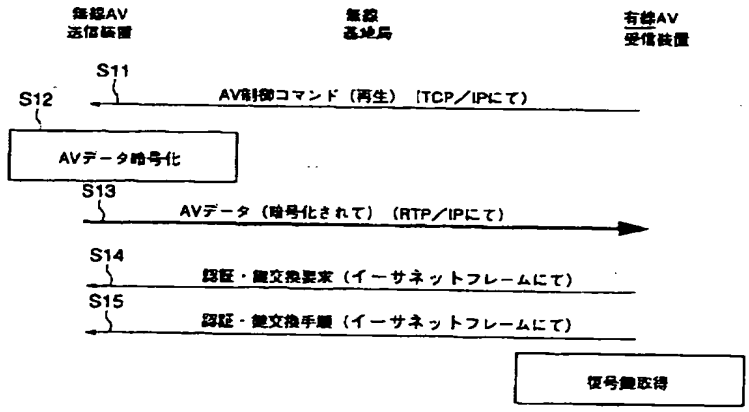
【図１１】


イーサネットヘッダ
認証・鍵交換用データ
プロトコルタイプ＝著作権保護プロトコル（例：DTCP）

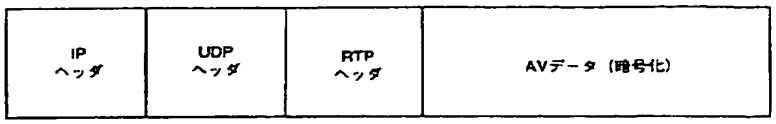
【図６】


無線AV
送信装置
無線
基地局
無線AV
受信装置
S1
AV制御コマンド（再生）（TCP／IPにて）
S2
AVデータ暗号化
S3
AVデータ（暗号化されて）（RTP／IPにて）
S4
認証・鍵交換要求（無線レイヤパケットにて）
S5
認証・鍵交換手順（無線レイヤパケットにて）
復号鍵取得

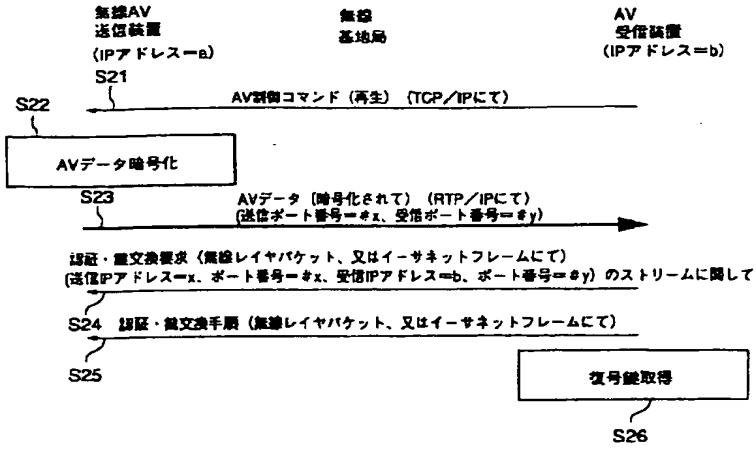
【図１２】


無線AV
送信装置
無線
基地局
有線AV
受信装置
S11
AV制御コマンド（再生）（TCP／IPにて）
S12
AVデータ暗号化
S13
AVデータ（暗号化されて）（RTP／IPにて）
S14
認証・鍵交換要求（イーサネットフレームにて）
S15
認証・鍵交換手順（イーサネットフレームにて）
復号鍵取得

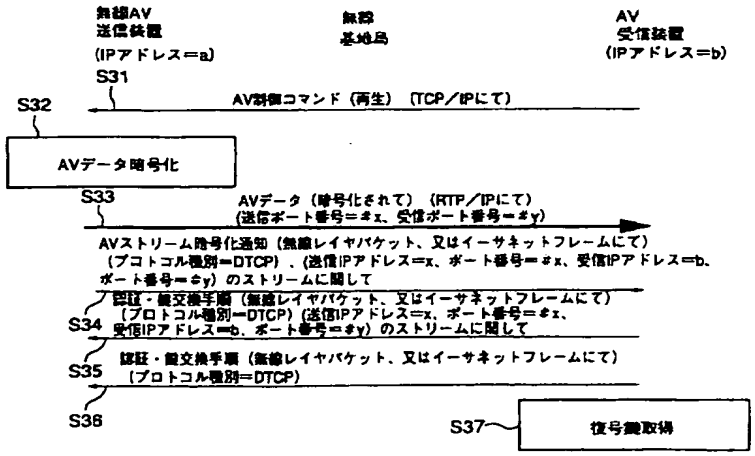
【図１５】


IP
ヘッダ
UDP
ヘッダ
RTP
ヘッダ
AVデータ（暗号化）

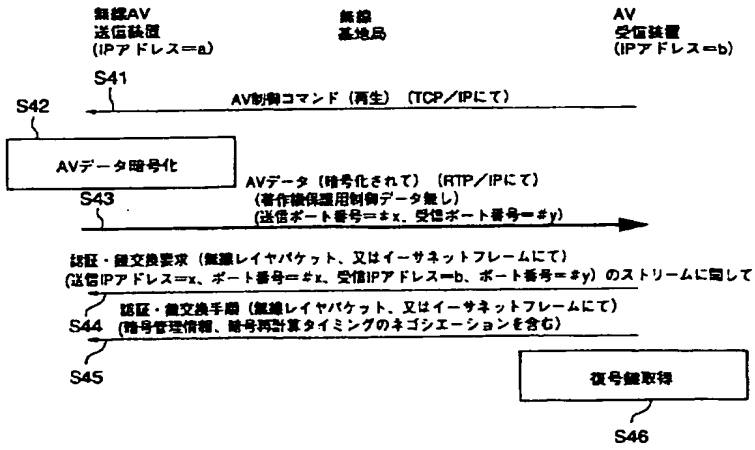
【図１３】


無線AV
送信装置
(IPアドレス=a)
無線
基地局
AV
受信装置
(IPアドレス=b)
S21
AV制御コマンド（再生）（TCP/IPにて）
S22
AVデータ暗号化
S23
AVデータ（暗号化されて）（RTP/IPにて）
(送信ポート番号=*x、受信ポート番号=*y)
認証・鍵交換要求（無線レイヤパケット、又はイーサネットフレームにて）
(送信IPアドレス=x、ポート番号=*x、受信IPアドレス=b、ポート番号=*y）のストリームに関して
S24 認証・鍵交換手順（無線レイヤパケット、又はイーサネットフレームにて）
S25
復号鍵取得
S26

【図１４】


無線AV
送信装置
(IPアドレス=a)
無線
基地局
AV
受信装置
(IPアドレス=b)
S31
AV制御コマンド（再生）（TCP/IPにて）
S32
AVデータ暗号化
S33
AVデータ（暗号化されて）（RTP/IPにて）
(送信ポート番号=*x、受信ポート番号=*y)
AVストリーム暗号化通知（無線レイヤパケット、又はイーサネットフレームにて）
（プロトコル種別=DTCP）、(送信IPアドレス=x、ポート番号=*x、受信IPアドレス=b、
ポート番号=*y）のストリームに関して
認証・鍵交換手順（無線レイヤパケット、又はイーサネットフレームにて）
S34 （プロトコル種別=DTCP）(送信IPアドレス=x、ポート番号=*x、
受信IPアドレス=b、ポート番号=*y）のストリームに関して
S35 認証・鍵交換手順（無線レイヤパケット、又はイーサネットフレームにて）
（プロトコル種別=DTCP）
S36
S37
復号鍵取得

【図１６】




フロントページの続き

(72)発明者　角田　啓治
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考)　5J104 AA07 EA02 EA15 KA01 KA04 NA02
5K033 AA08 BA01 CB11